**Journal of Information Security, 2016, 7, 29-48**
Published Online March 2016 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2016.72003

Scientific Research Publishing

# Empirical Investigation of Threats to Loyalty Programs by Using Models Inspired by the Gordon-Loeb Formulation of Security Investment

**Shiori Shinoda, Kanta Matsuura**

Institute of Industrial Science, The University of Tokyo, Tokyo, Japan
Email: shinoda.shiori@gmail.com, kanta@iis.u-tokyo.ac.jp

Received 26 December 2015; accepted 14 March 2016; published 17 March 2016





## Abstract

**Loyalty program (LP) is a popular marketing activity of enterprises. As a result of firms' effort to increase customers' loyalty, point exchange or redemption services are now available worldwide. These services attract not only customers but also attackers. In pioneering research, which first focused on this LP security problem, an empirical analysis based on Japanese data is shown to see the effects of LP-point liquidity on damages caused by security incidents. We revisit the empirical models in which the choice of variables is inspired by the Gordon-Loeb formulation of security investment: damage, investment, vulnerability, and threat. The liquidity of LP points corresponds to the threat in the formulation and plays an important role in the empirical study because it particularly captures the feature of LP networks. However, the actual proxy used in the former study is artificial. In this paper, we reconsider the liquidity definition based on a further observation of LP security incidents. By using newly defined proxies corresponding to the threat as well as other refined proxies, we test hypotheses to derive more implications that help LP operators to manage partnerships; the implications are consistent with recent changes in the LP network. Thus we can see the impacts of security investment models include a wider range of empirical studies.**

## Keywords

**Loyalty Program, Security Investment, Gordon-Loeb Model, Liquidity, Information Security Economics**

**How to cite this paper:** Shinoda, S. and Matsuura, K. (2016) Empirical Investigation of Threats to Loyalty Programs by Using Models Inspired by the Gordon-Loeb Formulation of Security Investment. *Journal of Information Security*, **7**, 29-48.
http://dx.doi.org/10.4236/jis.2016.72003

## 1. Introduction

Loyalty programs (LPs) are structured marketing efforts that reward, and therefore encourage, customers' loyalty [1]. LPs have proliferated in recent years as companies seek to acquire and retain customers, increase customer spending, and encourage the purchase of additional products [2]. However, some studies such as [3] argued that since most firms now utilize LPs, they are no longer effective in contributing to competitive advantage. Consequently, many firms are attempting to redesign LPs to enhance their effectiveness. In particular, in order to increase customers' loyalty, point exchange or redemption services have matured worldwide. For example, Points.com[1] is a major point exchange or redemption service in the U.S. In Japan, point exchange network is expanding, which enables customers to redeem points from one LP to another LP [4]. However, these services attract not only customers but also attackers whose aim is to obtain monetary benefits. In fact, there are an increasing number of LP incidents worldwide, as shown in Section 2.

When we consider security investment to reduce the damages caused by such incidents, we need to assess the features of LP network from the viewpoint of the efficacy of security investment. In order to answer to the above question, Jenjarrussakul and Matsuura [5] conducted an empirical study of LPs. Their study was performed inspired by the Gordon-Loeb model [6]-[8] of security investment; they considered damage, expense (or security investment), threat, and vulnerability as four fundamental factors when they developed their empirical analysis model. In particular, they provided security-liquidity implications by using the *liquidity* of an LP as a metric of threat. This analysis is possible because threat (defined as the probability of a threat occurring) and vulnerability (defined as the conditional probability that a threat once realized would be successful) are handled separately.

However, the definition of the liquidity itself is not deeply studied. The possibility of using other metrics is not well considered, either. In this paper, we investigate this threat metric more deeply by considering different metrics based on an observation of actual security incidents on LP systems.

Our work to be reported in the rest of this paper is inspired by this primary study [5], but there are important differences as follows. First, the liquidity definition is reconsidered, and a more intuitively convincing one is introduced. Second, we observe actual security incidents more deeply and give more implications that help LP operators to manage partnerships; the implications are consistent with recent changes in the LP network. Minor changes over the proxies used to test hypotheses also help our empirical study.

The rest of this paper is organized as follows. In Section 2, we see major incidents on LPs, which occurred worldwide, and their characteristics. In Section 3, we describe related and previous works. In Section 4, the data used in our empirical analyses are shown. In Sections 5, 6 and 7, different threat metrics and liquidity definition are investigated. Lastly, Section 8 concludes the paper.

## 2. Incidents on Loyalty Programs

In the U.K., compromised credentials enabled the theft of users' miles from the British Airways loyalty program in March 2015 [9]. In the U.S., Hilton Hotel rewards points were stolen in November 2014 [10]. This case happened because the login process was weak. Hackers can not only sell the stolen accounts or redeem the points but can also buy expensive items at Hilton shopping mall. About 10,000 accounts of American Airlines and United Airlines loyalty programs were compromised in December 2014 [11]. A March 2015 report [12] says "with Starbucks, hackers were somehow (still unclear) able to obtain customer usernames and passwords that opened up access to payment methods, which were used to refill gift card balances and transfer out gift card funds. Hackers can then sell these gift card balances to other people." In these cases, hackers are said to have used ID-password lists for mimicking successful authentications.

There is an increasing number of LP security incidents in Japan as well [13]. **Table 1** shows a list of major security incidents of LPs in Japan collected from web news articles that describe some characteristics of the attackers' behaviors: they often 1) attempt to go through the web login authentication mechanisms, 2) make malicious attempts in one or two days, and 3) attempt to steal the compromised accounts' points and redeem them into certain LP points. Regarding the third characteristic, it should be noted that Amazon Gift Card and iTunes Gift Code are often chosen as the redemption destinations by attackers. Their codes can be sold and eventually converted into real money. This is the first possible reason why attackers often choose those gifts. The second possible reason is that most attackers live outside Japan. Both Amazon and iTunes services are provided

[1]https://www.points.com/.

**Table 1.** Major LP security incidents in Japan.

| Date | LP | Redemption destination | # of malicious redemptions | Damage (USD) | Source |
|---|---|---|---|---|---|
| 2012.4.14-16 | G Point | Amazon Gift Card | 442 | 13,258 | [14] |
| 2013.3.26 | T Point | other accounts of T point | - | - | [15] |
| 2013.12 | Rakuten Super Point | electric money | - | 24,590 | [16] |
| 2014.1.19 | Potora | - | - | - | [17] |
| 2014.1.31-2.2 | JAL Mileage Bank | Amazon Gift Card | 65 | >20,000 | [18] |
| 2014.3 | Suica Point Club | - | - | - | [19] |
| 2014.2 | Hatena | Amazon Gift Card | - | - | [20] |
| 2014.3.7-9 | ANA Mileage Club | iTunes Gift Code | | 5,328 | [21] |
| 2014.3 | Oki Doki Point Program | T point | Some | - | [22] |
| 2014.4.19-29 | Sony Point | Playstation store ticket, mora music card ID | 273 | 6,172 | [23] |
| 2014.5.27-6.4 | niconico point | - | 19 | 1,423 | [24] |
| 2014.6.16-19 | Hatena | Amazon Gift Card | 0 (of 3 applications) | - | [25] |
| 2014.6.23 | CAPAT | - | 203 | - | [26] |
| 2014.7.4 | Anpara | - | 60 | - | [27] |
| 2014.7.11-28 | Poin-talk | prizes, other point programs | 568 | 4,918 | [28] |
| 2014.8 | Suica Point Club | - | - | - | [29] |
| 2014.1 | D STYLE WEB | - | 47 | - | [30] |
| 2014.11 | Hearcon | - | 291 | - | [31] |
| 2014.12.23 | morappo (mixi) | - | 332 | 3,566 | [32] |
| 2015.5.17-6.29 | AIP | - | 33 | 1,228 | [33] |
| 2015.7.4-6 | Life Media | Amazon Gift Card, iTunes Gift Code | 0 (of 25 applications) | 0 | [34] |
| 2015.7 | Orico Point | T Point | 156 | - | [35] |
| 2015.7.11 | Prize Prize | Point-on PON | Some | - | [36] |
| 2015.8.4 | Lodging Net Point | Amazon Gift Card | 123 | 2,418 | [37] |

internationally with their head offices outside Japan, so attackers can avoid investigations by Japanese police. As the third possible reason, it should be noted that Amazon and iTunes are not willing to publish the redemption algorithms; without their disclosure, we cannot trace and find who stole the points.

## 3. Related Works

### 3.1. Loyalty Programs

Effectiveness of LPs is well investigated in the management area [3]. Also, some research focuses on Japanese LPs. For example, the research has been conducted on the characteristics of Japanese LP network [38], the factor which leads LP partnership [39], LP network's economic reliability [40] and the network's impact on marketing performances [4]. These works do not consider LP security problems.

LP security issues were first economically researched by Jenjarrussakul and Matsuura in 2014 [5]. They show two implications: the impact of LP security incidents gets lower if stronger security requirements in web authen-

tication process are satisfied, and it is higher if the liquidity of the LP points gets higher. Our work is inspired by this primary study, but there are some important differences as mentioned in Section 1.

### 3.2. Virtual Currency and Security

European Central Bank defined virtual currency as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" and pointed out that LP points or miles can satisfy the definition [41]. Other representative virtual currencies include cryptocurrency and game currency. Regarding cryptocurrency, Bitcoin is the main research target [42]-[45]. Although these works handle security problems, they do not consider the relation between Bitcoin and LP systems. Massively multiplayer online games (MMOGs) currencies are also virtual currencies with security issues that have been researched without considering the relationship between the currencies and LP systems [46]-[50].

## 4. Data Collection

We retrieved the LP network structure from Poitan.net, a portal site of Japanese LP networks where users can search possible routes of point redemption, find the market value of each LP point, and so on (see **Appendix A.1**). Each LP operator's capital size was retrieved from each LP operator's website. The data of the security investment, damage amount and security requirements are the same as those in [5]. **Table 2** summarizes the data used in our study.

## 5. Point Liquidity and Number of Partners

### 5.1. Hypothesis Development

Reference [5] shows an important implication: an LP with higher liquidity suffers a bigger impact from incidents. However, the definition of the liquidity in [5] was not intuitively convincing as described in **Appendix C**. It may be more convincing if *liquidity* is defined more simply as:

$$liquidity_i = GoPartner_i \tag{1}$$

where $GoPartner_i$ is the number of partners into which one can redeem points from $LP_i$. In order to examine this definition, we set the following hypothesis:

*H*1. *An LP with more outgoing partners suffers greater damage*.

### 5.2. Model

In order to test *H*1, the following linear regression model is set:

$$\frac{\log(damage_i)}{\log(capital_i)} = \beta_0 + \beta_1 \frac{\log(expense_i)}{\log(capital_i)} + \beta_2 GoPartner_i + \beta_3 sec\_score_i + u_i \tag{2}$$

where $i$ is an index that indicates each LP, $damage_i$ is the annual damage amount of the overall IT security

**Table 2.** Data used in our study.

| Data | Details |
|---|---|
| LPs | 82 Japanese LPs, which were selected by Jenjarrussakul and Matsuura [5] among 207 Japanese LPs registered at Poitan.net in Feb. 2014. For details, see **Appendix B.1**. |
| Security investment and damage amount of security incident | Retrieved from Information Processing Census (2012), the statistical data by METI (Ministry of Economics, Technology and Industries) of Japan [51]. |
| Exchange network | Retrieved at Poitan.net in Dec. 2014. |
| Security requirement | Retrieved by Jenjarrussakul and Matsuura [5] in Apr. 2014; they investigated security requirements in each process of registration, login authentication and back-up authentication. For more details, see **Appendix B.3.3**. |
| Capital size | Retrieved from every LP operator's web page in Feb. 2015. Each capital size is shown in **Appendix B.1**. |

incidents of $LP_i$'s operator, $capital_i$ is the capital size of $LP_i$'s operator, $expense_i$ is the annual IT security expense of $LP_i$'s operator, $sec\_score_i$ is the security requirement level of the $LP_i$'s authentications, and $u_i$ is the model's error term, assumed to be independent of the observed covariates. For more calculation details of these proxies, see **Appendix B.3**. Correlations between variables are shown in **Table 3**.

### 5.3. Results

To test $H1$, let the null hypothesis be $\beta_2 = 0$ in Equation (2). $H1$ is accepted if this null hypothesis is rejected.

The estimated result of Equation (2) is shown in **Table 4**. The coefficient of $GoPartner_i$ is significantly positive, so the null hypothesis $\beta_2 = 0$ is rejected, and $H1$ is accepted. Additionally, the coefficient of $sec\_score_i$ is significantly negative. This result is consistent with the results of [5].

## 6. Does Time Required for Redemption Affect the Damage?

### 6.1. Hypothesis Development

A redemption request is not always approved quickly; it may take one week or longer. If the LP operators have more time to give approval, they may notice suspicious redemption applications and reject them with higher chances. Thus attackers may prefer quicker redemption to avoid the risk of being detected. In fact, the incidents surveyed in Section 2 suggest this preference. So let us consider the following hypothesis.

*H*2. *If an LP has more outgoing partners with short redemption time*, *the damage from incidents is bigger*.

### 6.2. Data and Descriptive Statistics

**Figure 1** shows the histogram of the time required for redemptions of all the exchange routes of 274 LPs and **Table 5** shows the descriptive statistics. **Table 6** shows the descriptive statistics regarding the 82 selected LPs.

### 6.3. Model

To test $H2$, we set the linear regression model as follows:

$$\frac{\log\left(damage_i\right)}{\log\left(capital_i\right)} = \beta_0 + \beta_1 \frac{\log\left(expense_i\right)}{\log\left(capital_i\right)} + \beta_2 GoPartner_{i,N} + \beta_3\left(GoPartner_{i,90} - GoPartner_{i,N}\right) + \beta_4 sec\_score_i + u_i \tag{3}$$

**Table 3.** Correlations between the variables in Equation (2). To save space, the following notation is used: ldam is $\log(damage_i)$, lcap is $\log(capital_i)$, lex is $\log(expense_i)$, GoPartner is $GoPartner_i$, and SecScore is $sec\_score_i$.

| | *ldam/lcap* | *lex/lcap* | *GoPartner* | *SecScore* |
|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - |
| *GoPartner* | 0.204 | 0.090 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | 0.025 | 1.000 |

**Table 4.** Results of the linear regression by Equation (2). The notations are the same as in **Table 3**.

| Variable | Coef. | Std. Err | Prob. | |
|---|---|---|---|---|
| C | −0.218 | 0.091 | 0.020 | ** |
| *lex/lcap* | 1.107 | 0.117 | 0.000 | *** |
| *GoPartner* | 0.002 | 0.001 | 0.029 | ** |
| *SecScore* | −0.054 | 0.019 | 0.006 | *** |
| Adj. $R^2$ | 0.677 | | | |

**Indicates significance at 5% level. ***Indicates significance at 1% level.

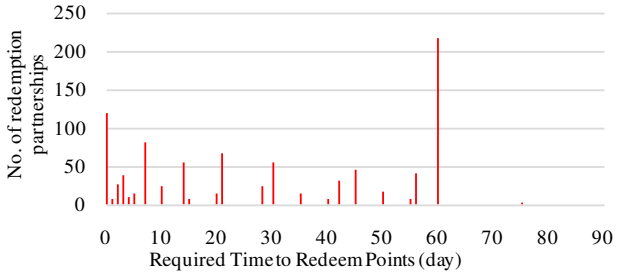


**Figure 1.** Histogram of the time required for redemption in December 2014.

**Table 5.** Descriptive statistics of the time reqiured for redemption.

| # of nodes | Min | Max | 1st Quartile | 3rd Quartile | Mean | Median |
|---|---|---|---|---|---|---|
| 1265 | 0 | 90 | 7 | 56 | 30 | 28 |

**Table 6.** Descriptive statistics of the number of outgoing partners regarding the 82 selected LPs. $Go_N$represents the number of partners into which one can redeem points from each LP within $N$ days.

| | Min | Max | 1st Quar. | Median | 3rd Quar. | Ave. | Std. Dev. |
|---|---|---|---|---|---|---|---|
| $Go_0$ | 0 | 9 | 0 | 0 | 1 | 0.890 | 1.61 |
| $Go_5$ | 0 | 16 | 0 | 1 | 2 | 1.77 | 2.79 |
| $Go_{10}$ | 0 | 19 | 0 | 1 | 3 | 2.44 | 3.72 |
| $Go_{20}$ | 0 | 19 | 0 | 1 | 3 | 2.44 | 3.72 |
| $Go_{30}$ | 0 | 26 | 0 | 2 | 4 | 3.15 | 4.54 |
| $Go_{45}$ | 0 | 37 | 0 | 2 | 7 | 4.55 | 6.41 |
| $Go_{60}$ | 0 | 39 | 1 | 3 | 9 | 6.33 | 7.85 |
| $Go_{90}$ | 0 | 40 | 1 | 3 | 9 | 6.50 | 7.94 |

where $GoPartner_{i,N}$ is the number of partners into which one can redeem points from $LP_i$ within $N$ days and the other variables are the same as those in Equation (2). Correlations between variables are shown in **Table7**.

### 6.4. Results and Discussion

The estimated results of Equation (3) for $N = 0,5,10,30,45,60$ are shown in **Table 8**. When $N$ is 0 or 5, $\beta_3$ is significantly positive, but $\beta_2$ does not show any significances. This means that if an LP suffers greater damage if it has more point-redeeming partners over the time threshold, 0 or 5 days. On the other hand, when $N$ is 45 or 60, $\beta_3$ shows no significance but $\beta_2$ is significantly positive. This suggests that a LP suffers more damage when it has a larger number of point-redeeming partners under the time threshold, 45 or 60 days. When $N$ is 10 or 30, no significances were provided.

These results suggest that the number of outgoing partners that require at least 45 days for redemption does not affect the liquidity. Although it is not supported if the threshold time is 5 days, $H2$ is supported if the threshold time is 45 days. It is shown that the damage gets bigger if the LP has more partnerships with shorter redemption times. Thus we find that redemption time has some effects on liquidity, and hence, on the threats to LPs.

## 7. Do Specific Partners Affect the Damage?

### 7.1. Hypothesis Development

**Table 9** and **Figure 2** show the number of LPs (out of the 82 selected LPs) from which one can redeem points

**Table 7.** Correlations between the variables in Equation(3) for different values of $N$. $Go_N$ represents $GoPartner_{i.N}$ and other notations are the same as in **Table 3**.

(a) $N = 0$

| | *ldam/lcap* | *lex/lcap* | $Go_0$ | $Go_{90}$-$Go_0$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $Go_0$ | 0.273 | 0.247 | 1.000 | - | - |
| $Go_{90}$-$Go_0$ | 0.164 | 0.044 | 0.380 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.314 | 0.058 | 1.000 |

(b) $N = 5$

| | *ldam/lcap* | *lex/lcap* | $Go_5$ | $Go_{90}$-$Go_5$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $Go_5$ | 0.223 | 0.255 | 1.000 | - | - |
| $Go_{90}$-$Go_5$ | 0.152 | 0.000 | 0.333 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.192 | 0.112 | 1.000 |

(c) $N = 10$

| | *ldam/lcap* | *lex/lcap* | $Go_{10}$ | $Go_{90}$-$Go_{10}$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $Go_{10}$ | 0.320 | 0.265 | 1.000 | - | - |
| $Go_{90}$-$Go_{10}$ | 0.075 | −0.047 | 0.379 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.184 | 0.153 | 1.000 |

(d) $N = 30$

| | *ldam/lcap* | *lex/lcap* | $Go_{30}$ | $Go_{90}$-$Go_{30}$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $Go_{30}$ | 0.289 | 0.210 | 1.000 | - | - |
| $Go_{90}$-$Go_{30}$ | −0.001 | −0.121 | 0.379 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.100 | 0.196 | 1.000 |

(e) $N = 45$

| | *ldam/lcap* | *lex/lcap* | $Go_{45}$ | $Go_{90}$-$Go_{45}$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $Go_{45}$ | 0.294 | 0.171 | 1.000 | - | - |
| $Go_{90}$-$Go_{45}$ | −0.081 | −0.117 | 0.278 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.088 | 0.234 | 1.000 |

(f) $N = 60$

| | *ldam/lcap* | *lex/lcap* | $Go_{60}$ | $Go_{90}$-$Go_{60}$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $Go_{60}$ | 0.204 | 0.090 | 1.000 | - | - |
| $Go_{90}$-$Go_{60}$ | 0.034 | 0.006 | 0.123 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | 0.021 | 0.063 | 1.000 |

**Table 8.** Results of the regression by Equation (3) for $N = 0, 5, 10, 30, 45, 60$. The notations are the same as in **Table 7**.

| | $N = 0$ | | | | $N = 5$ | | | | $N = 10$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Variable | Coef. | Std. Err | Prob. | | Coef. | Std. Err | Prob. | | Coef. | Std. Err | Prob. | |
| C | −0.219 | 0.093 | 0.0212 | ** | −0.238 | 0.0908 | 0.0106 | ** | −0.221 | 0.0931 | 0.0202 | ** |
| *lex/lcap* | 1.11 | 0.119 | 0.000 | *** | 1.14 | 0.116 | 0.000 | *** | 1.11 | 0.120 | 0.000 | *** |
| $Go_N$ | 0.00148 | 0.00475 | 0.763 | | −0.00259 | 0.00268 | 0.337 | | 0.00147 | 0.00212 | 0.489 | |
| $Go_{90}$-$Go_N$ | 0.00197 | 0.00103 | 0.0607 | * | 0.00316 | 0.0011 | 0.0054 | *** | 0.00214 | 0.0133 | 0.110 | |
| *SecScore* | −0.0543 | 0.0192 | 0.0061 | *** | −0.0602 | 0.0191 | 0.0023 | *** | −0.0550 | 0.0195 | 0.0063 | *** |
| Adj. $R^2$ | 0.677 | | | | 0.690 | | | | 0.677 | | | |

| | $N = 30$ | | | | $N = 45$ | | | | $N = 60$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Variable | Coef. | Std. Err | Prob. | | Coef. | Std. Err | Prob. | | Coef. | Std. Err | Prob. | |
| C | −0.222 | 0.0934 | 0.0199 | ** | −0.209 | 0.0919 | 0.0261 | ** | −0.217 | 0.0919 | 0.0206 | ** |
| *lex/lcap* | 1.11 | 0.120 | 0.000 | *** | 1.09 | 0.118 | 0.000 | *** | 1.11 | 0.117 | 0.000 | *** |
| $Go_N$ | 0.00162 | 0.00137 | 0.242 | | 0.00259 | 0.00113 | 0.0253 | ** | 0.00187 | 0.000881 | 0.0367 | ** |
| $Go_{90}$-$Go_N$ | 0.00241 | 0.00199 | 0.230 | | −9.98E−06 | 0.000227 | 0.997 | | 0.00467 | 0.0122 | 0.704 | |
| *SecScore* | −0.0550 | 0.0194 | 0.006 | *** | −0.0503 | 0.0195 | 0.0118 | ** | −0.0544 | 0.0192 | 0.0059 | *** |
| Adj. $R^2$ | 0.677 | | | | 0.680 | | | | 0.677 | | | |

*Indicates significance at 10% level. **Indicates significance at 5% level. ***Indicates significance at 1% level.

**Table 9.** Number of LPs (out of the 82 selected LPs) from which one can redeem points into Amazon and iTunes for $N = 0, 5, 10, 30, 45, 60, 90$.

| | $N = 0$ | $N = 5$ | $N = 10$ | $N = 30$ | $N = 45$ | $N = 60$ | $N = 90$ |
|---|---|---|---|---|---|---|---|
| Amazon | 4 | 6 | 10 | 14 | 15 | 16 | 17 |
| iTunes | 3 | 5 | 9 | 14 | 14 | 15 | 16 |
| Amazon or iTunes | 5 | 7 | 11 | 16 | 17 | 19 | 20 |
| Amazon and iTunes | 2 | 4 | 8 | 12 | 12 | 12 | 13 |

into Amazon Gift Cards and iTunes Gift Codes with respect to the time required for redemption. As we mentioned in Section 2, attackers seem to prefer Amazon Gift Cards and iTunes Gift Codes for malicious redemptions. Taking alliances with specific partners might expose an LP to bigger threats. So we set the following hypothesis.

*H3. An LP that takes partnership with Amazon or iTunes suffers greater damage.*

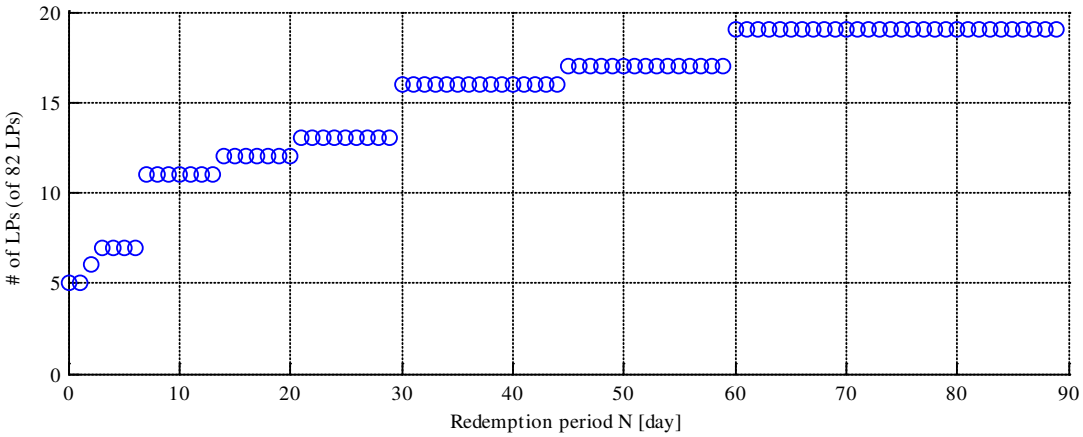


**Figure 2.** Number of LPs (of the 82 selected LPs) from which one can redeem into Amazon Gift Card or iTunes Gift Code within *N* days.

## 7.2. Model

To test *H*3, we set the linear regression model as follows:

$$\frac{\log(damage_i)}{\log(capital_i)} = \beta_0 + \beta_1 \frac{\log(expense_i)}{\log(capital_i)} + \beta_2 GoToAorI_{i,N} + \beta_3 \left(GoToAorI_{i,90} - GoToAorI_{i,N}\right) + \beta_4 sec\_score_i + u_i \quad (4)$$

when $N < 90$, and

$$\frac{\log(damage_i)}{\log(capital_i)} = \beta_0 + \beta_1 \frac{\log(expense_i)}{\log(capital_i)} + \beta_2 GoToAorI_{i,90} + \beta_3 sec\_score_i + u_i \quad (5)$$

when $N = 90$, where $GoToAorI_{i,N}$ is the binary value representing whether one can redeem points from $LP_i$ to an Amazon Gift Card or iTunes Gift Code within $N$ days (1 if possible, 0 otherwise), and the other variables are the same as in Equation (2).

Correlations between the variables in Equation (4) and Equation (5) are shown in **Table 10**.

## 7.3. Results and Discussion

The estimated results for $N = 0, 5, 10, 30, 45, 60, 90$ are shown in **Table 11**.

When $N = 10, 45, 90$, $\beta_2$ is significantly weakly positive at 10% level. When *N* is 10 or 45, $\beta_3$ does not show any significance. This means that *H*3 is weakly supported for the redemption time, 10, 45 and 90 days. Additionally, it suggests that availability of redemption into Amazon or iTunes does not affect the damage if one has to wait more than 45 days to complete the transaction. When *N* = 30 or *N* = 60, the p-values of $\beta_2$ are rather small, although it is insufficient for the 10%-level weak support. On the other hand, when *N* = 0 or *N* = 5, $\beta_3$ is significantly positive and $\beta_2$ is insignificant. This means if an LP has an outgoing partnership with Amazon or iTunes and the redemption takes more than 0 or 5 days, it suffers more damage, while we cannot see any relation between the damage and the availability of 0 or 5-day redemption. While it differs from the intuition, the same discussion as in Section 6.4 can be applied.

In Japan, some of the LP operators who experienced damages by malicious redemption into Amazon Gift Cards or iTunes Gift Codes introduced countermeasures; they either temporarily stopped their alliance with Amazon and iTunes or introduced phone authentication regarding the redemption into. This recent trend is supported by the above result of our empirical analysis.

# 8. Concluding Remarks

In this paper, we revisit the empirical models used in a former study [5] regarding the security of loyalty

**Table 10.** Correlations between variables in Equations (4) and (5) for different values of $N$. GoAI$_N$ represents $GoToAorI_{i,N}$ and other notations are the same as in **Table 3**.

(a) $N = 0$

| | *ldam/lcap* | *lex/lcap* | $GoAI_0$ | $GoAI_{90}$-$GoAI_0$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $GoAI_0$ | −0.054 | −0.019 | 1.000 | - | - |
| $GoAI_{90}$-$GoAI_0$ | 0.488 | 0.385 | −0.126 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.055 | −0.361 | 1.000 |

(b) $N = 5$

| | *ldam/lcap* | *lex/lcap* | $GoAI_5$ | $GoAI_{90}$-$GoAI_5$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $GoAI_5$ | 0.007 | 0.073 | 1.000 | - | - |
| $GoAI_{90}$-$GoAI_5$ | 0.476 | 0.339 | −0.138 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.149 | −0.304 | 1.000 |

(c) $N = 10$

| | *ldam/lcap* | *lex/lcap* | $GoAI_{10}$ | $GoAI_{90}$-$GoAI_{10}$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $GoAI_{10}$ | 0.320 | 0.234 | 1.000 | - | - |
| $GoAI_{90}$-$GoAI_{10}$ | 0.212 | 0.205 | −0.144 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.243 | −0.224 | 1.000 |

(d) $N = 30$

| | *ldam/lcap* | *lex/lcap* | $GoAI_{30}$ | $GoAI_{90}$-$GoAI_{30}$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $GoAI_{30}$ | 0.296 | 0.259 | 1.000 | - | - |
| $GoAI_{90}$-$GoAI_{30}$ | 0.271 | 0.193 | −0.116 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.243 | −0.263 | 1.000 |

(e) $N = 45$

| | *ldam/lcap* | *lex/lcap* | $GoAI_{45}$ | $GoAI_{90}$-$GoAI_{45}$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $GoAI_{45}$ | 0.377 | 0.296 | 1.000 | - | - |
| $GoAI_{90}$-$GoAI_{45}$ | 0.123 | 0.129 | −0.104 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.272 | −0.226 | 1.000 |

(f) $N = 60$

| | *ldam/lcap* | *lex/lcap* | $GoAI_{60}$ | $GoAI_{90}$-$GoAI_{60}$ | *SecScore* |
|---|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - | - |
| $GoAI_{60}$ | 0.391 | 0.321 | 1.000 | - | - |
| $GoAI_{90}$-$GoAI_{60}$ | 0.100 | 0.083 | −0.064 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.329 | −0.129 | 1.000 |

(g) $N = 90$

| | *ldam/lcap* | *lex/lcap* | $GoAI_{90}$ | *SecScore* |
|---|---|---|---|---|
| *ldam/lcap* | 1.000 | - | - | - |
| *lex/lcap* | 0.790 | 1.000 | - | - |
| $GoAI_{90}$ | 0.410 | 0.336 | 1.000 | - |
| *SecScore* | −0.491 | −0.417 | −0.357 | 1.000 |

**Table 11.** Results of the linear regression by Equations (4) and (5) for $N = 0, 5, 10, 30, 45, 60, 90$. The notations are the same as in **Table 10**.

| | $N = 0$ | | | | $N = 5$ | | | | $N = 10$ | | | | $N = 30$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Variable | Coef. | Std. Err | Prob. | | Coef. | Std. Err | Prob. | | Coef. | Std. Err | Prob. | | Coef. | Std. Err | Prob. | |
| C | −0.179 | 0.0930 | 0.0585 | * | −0.179 | 0.0910 | 0.053 | * | −0.205 | 0.0936 | 0.0318 | ** | −0.205 | 0.0936 | 0.0318 | ** |
| *lex/lcap* | 1.05 | 0.120 | 0.000 | *** | 1.05 | 0.117 | 0.000 | *** | 1.09 | 0.121 | 0.000 | *** | 1.09 | 0.121 | 0.000 | *** |
| $GoAI_N$ | −0.0120 | 0.0284 | 0.674 | | −0.0137 | 0.0244 | 0.575 | | 0.0389 | 0.0215 | 0.0749 | * | 0.0247 | 0.0185 | 0.186 | |
| $GoAI_{90}$-$GoAI_N$ | 0.0468 | 0.0196 | 0.0197 | ** | 0.0557 | 0.0200 | 0.0067 | *** | 0.018 | 0.0233 | 0.441 | | 0.0523 | 0.0337 | 0.125 | |
| *SecScore* | −0.0405 | 0.0196 | 0.0425 | ** | −0.0423 | 0.0192 | 0.0311 | ** | −0.0428 | 0.0199 | 0.0351 | ** | −0.0407 | 0.0201 | 0.0465 | ** |
| Adj. $R^2$ | 0.682 | | | | 0.693 | | | | 0.670 | | | | 0.671 | | | |

| | $N = 45$ | | | | $N = 60$ | | | | $N = 90$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Variable | Coef. | Std. Err | Prob. | | Coef. | Std. Err | Prob. | | Coef. | Std. Err | Prob. | |
| C | −0.203 | 0.0937 | 0.0338 | ** | −0.205 | 0.0940 | 0.0322 | ** | −0.205 | 0.0933 | 0.031 | ** |
| *lex/lcap* | 1.09 | 0.121 | 0.000 | *** | 1.09 | 0.121 | 0.000 | *** | 1.09 | 0.120 | 0.000 | *** |
| $GoAI_N$ | 0.0331 | 0.0183 | 0.0741 | * | 0.0295 | 0.0178 | 0.102 | | 0.0295 | 0.0175 | 0.0958 | * |
| $GoAI_{90}$-$GoAI_N$ | 0.00578 | 0.0380 | 0.880 | | 0.0282 | 0.0634 | 0.657 | | N/A | N/A | N/A | |
| *SecScore* | −0.0444 | 0.0201 | 0.0302 | ** | −0.0427 | 0.0201 | 0.0365 | ** | −0.0427 | 0.0199 | 0.035 | ** |
| Adj. $R^2$ | 0.670 | | | | 0.668 | | | | 0.668 | | | |

*Indicates significance at 10% level. **Indicates significance at 5% level. ***Indicates significance at 1% level.

programs. In the models, the choice of variables is inspired by the Gordon-Loeb formulation of security investment: damage, investment, vulnerability, and threat. The liquidity of LP points corresponds to the threat in the formulation and plays an important role in the empirical study because it captures a particular feature of LP networks. However, the actual proxy used in the former study is artificial due to the fact that its original definition is not LP-wise but industry-wise. In this paper, we reconsidered the liquidity definition based on a further

observation of LP security incidents. By using newly defined proxies corresponding to the threat as well as other refined proxies, we conducted hypothesis testing to derive more implications. We show the damage from LP incidents grows if partnerships with short redemption times or with Amazon or iTunes are accepted. These implications will help LP operators manage partnerships. In fact, these findings are consistent with recent trends in the LP network. Thus we can see the impacts of security investment models include a wider range of empirical studies in the economics of information security.

## Acknowledgements

We thank the editors and the referees for their helpful comments. This work was partly supported by JSPS KAKENHI Grant Number 25280045 and 25240017. The authors express sincere appreciation to Mr. Takahito Kikuchi, the owner of Poitan.net, who provided the data and useful information for this study.

## References

[1] Sharp, B. and Sharp, A. (1997) Loyalty Programs and Their Impact on Repeat-Purchase Loyalty Patterns. *International Journal of Research in Marketing*, **14**, 473-486. http://dx.doi.org/10.1016/S0167-8116(97)00022-0

[2] PricewaterhouseCoopers LLP (2013) Loyalty Analytics Exposed: What Every Program Manager Needs to Know. http://www.pwc.com/en_US/us/insurance/publications/assets/pwc-loyalty-analytics-exposed.pdf

[3] Zhang, J. and Breugelmans, E. (2012) The Impact of an Item-Based Loyalty Program on Consumer Purchase Behavior. *Journal of Marketing Research*, **49**, 50-65. http://dx.doi.org/10.1509/jmr.09.0211

[4] Katsumata, S. and Wakabayashi, T. (2014) Loyalty Program Point Exchange Networks and Their Impact on Marketing Performance. *Faculty of Economics*, *Nagasaki University Discussion Paper Series*, **2014**, 1-19.

[5] Jenjarrussakul, B. and Matsuura, K. (2014) Analysis of Japanese Loyalty Programs Considering Liquidity, Security Efforts, and Actual Security Levels. *The* 13*th Workshop on the Economics of Information Security*, Pennsylvania, 23-24 June 2014.

[6] Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, **5**, 438-457. http://dx.doi.org/10.1145/581271.581274

[7] Willemson, J. (2006) On the Gordon & Loeb Model for Information Security Investment. *The* 5*th Workshop on the Economics of Information Security*, Cambridge, 26-28 June 2006.

[8] Matsuura, K. (2008) Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. *The* 7*th Workshop on the Economics of Information Security*, New Hampshire, 25-28 June 2008.

[9] DarkReading.com (2015) British Airways the Latest Loyalty Program Breach Victim. http://www.darkreading.com/attacks-breaches/british-airways-the-latest-loyalty-program-breach-victim/d/d-id/1319683

[10] Krebs on Security (2014) Thieves Cash out Rewards, Points Accounts. http://krebsonsecurity.com/2014/11/thieves-cash-out-rewards-points-accounts/

[11] The Dallas Morning News (2015) Cyberthieves Steal Miles from American, United Customers. http://www.dallasnews.com/business/airline-industry/20150112-american-united-airlines-targets-of-attempt-to-steal-customers-miles.ece

[12] My Bank Tracker (2015) Lesson from Starbucks: Creative Ways That Hackers Can Steal from You. http://www.mybanktracker.com/news/lesson-starbucks-creative-ways-hackers-steal

[13] TrendMicro (2014) TrendLabs 2Q 2014 Security Roundup in Japan. (In Japanese) http://www.trendmicro.co.jp/cloud-content/jp/pdfs/security-intelligence/threat-report/pdf-2014q2-20140819.pdf?cm_sp=threat-_-sr-2014q2-_-lp-txt

[14] G-PLAN INC (2012) Correspondence to the Unauthorized Accesses to G-Point. (In Japanese) http://www.gpoint.co.jp/company/service/gplan20120418.pdf

[15] ITmedia Enterprise (2013) Unauthorized Access to T-Point, 299 Accounts Were Compromised. (In Japanese) http://www.itmedia.co.jp/enterprise/articles/1304/07/news005.html

[16] Record China (2013) Chinese Students Were Arrested. They Exchanged 250 Accounts Rakuten Points into Electric Money. (In Japanese) http://www.recordchina.co.jp/a80323.html

[17] NTT Communications Online Marketing Solutions (2014) The Report of Unauthorized Access to Potora. (In Japanese) http://www.nttcoms.com/page.jsp?id=2409

[18] ITpro (2014) Unauthorized Access to JAL Mileage Website, JAL Requested 27 Million People to Change Their Passwords. (In Japanese) http://itpro.nikkeibp.co.jp/article/NEWS/20140203/534282/

[19] Nikkei (2014) Enormous Unauthorized Access Attempted to JR East. (In Japanese) http://itpro.nikkeibp.co.jp/atcl/news/14/081800465/

[20] Hatena Co., Ltd. (2014) Please Confirm Your Password and Registration Information in Order to Prevent Unauthorized Access. (In Japanese) http://hatena.g.hatena.ne.jp/hatena/20140224/1393211701

[21] ITpro (2014) 1.12 Million Miles of ANA Mileage Club Were Stolen, Personal Information Such as Addresses Might Be Browsed. (In Japanese) http://itpro.nikkeibp.co.jp/article/NEWS/20140311/542563/

[22] Poitan News (2014) Unauthorized Access to My JCB and Redeemed to T-Point. (In Japanese) http://www.poitan.jp/archives/3138

[23] Sony Marketing (Japan) Inc. (2014) The Report of Unauthorized Access to Sony Point Service and a Request for Changing Passwords. (In Japanese) https://www.sony.jp/info/pw_management2.html

[24] Security NEXT (2014) 0.22 Million Unauthorized Accesses to Niconico Video, 0.17 Million Yen Loss. (In Japanese) http://www.security-next.com/049575

[25] Security NEXT (2014) Unauthorized Access to Hatena, Redemption to Amazon Gift Code Was Failed in Attempts. (In Japanese) http://www.security-next.com/049827

[26] Security NEXT (2014) 11502 Unauthorized Accesses to a Questionnaire Website and Some Points Were Stolen. (In Japanese) http://www.security-next.com/049982

[27] Scan Net Security (2014) A Questionnaire Website, Anpara, Was Attacked and Some Points Were Stolen. (In Japanese) http://scan.netsecurity.ne.jp/article/2014/07/08/34495.html

[28] NTT Communications Corporation (2014) Unauthorized Access to Poin-Talk and Goo-Points. (In Japanese) http://www.ntt.com/release/monthNEWS/detail/20140730.html

[29] ITpro (2014) Enormous Number of Accesses to Suica Point Club, Unauthorized Access to Some Acounts. (In Japanese) http://itpro.nikkeibp.co.jp/atcl/news/14/081800465/

[30] D Style Web (2014) Information of Unauthorized Access and Unauthorized Point Redemption. (In Japanese) http://www.dstyleweb.com/20141028/

[31] Security NEXT (2014) Unauthorized Access to a Research Service of Kyushu Electric Power, Which Was Detected When the Operator Found the Number of Exchanges Is 10 Times as Many as Usual. (In Japanese) http://www.security-next.com/054803

[32] Mixi, Inc. (2015) The Report of Unauthorized Accesses to Morappo and Mixi Questionnaire Using the Passwords Which Were Leaked at the Third Party. (In Japanese) http://mixi.co.jp/press/2015/0109/15881/

[33] AIP Corporation (2015) Unauthorized Access, Point Redemption and Personal Information Browsing. (In Japanese) http://www.aip-global.com/JP/corporate/releases/20150701.html

[34] Lifemedia, Inc. (2015) The Report of Unauthorized Access to Lifemedia. (In Japanese) http://lifemedia.jp/utilization/info_d20150713.html

[35] Orient Corporation (2015) Unauthorized Access to Customer Web Services. (In Japanese) http://www.orico.co.jp/information/20150727.html

[36] PrizePrize (2015) The Report of Unauthorized Point Redemptions and Our Request for Changing Your Passwords. (In Japanese) http://www.moneyforall.net/rss/single.php?id=121

[37] Washington Hotel (2015) The Report of Unauthorized Access to Lodging Net Point and Our Request for Changing Your Password. (In Japanese) http://www.washingtonhotel.co.jp/pdf/info20150805.pdf

[38] Wakabayashi, T. (2008) Structure and Formation of the Exchange Market of Point Programs and Electronic Moneys. (In Japanese) *Organizational Science*, **42**, 47-60.

[39] Wakabayashi, T. and Katsumata, S. (2013) Which Factor Matters to the Formation of Strategic Alliance Network: Industry, Firm or Network? (In Japanese) *Oganizational Science*, **47**, 69-79.

[40] Yuhashi, H. and Gotou, H. (2010) The Reliability of the New Economic Platform: Mobile Value Exchange Alliance Network. 18*th Biennial ITS Conference*, Tokyo, 27-30 June 2010.

[41] European Central Bank (2012) Virtual Currency Schemes. http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[42] Moore, T. and Christin, N. (2013) Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. *Financial Cryptography and Data Security*, **7859**, 25-33. http://dx.doi.org/10.1007/978-3-642-39884-1_3

[43] Vasek, M., Thornton, M. and Moore, T. (2014) Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. *Financial Cryptography and Data Security*, **8438**, 57-71. http://dx.doi.org/10.1007/978-3-662-44774-1_5

[44] Johnson, B., Laszka, A., Grossklags, J., Vasek, M. and Moore, T. (2014) Game-Theoretic Analysis of DDoS Attacks

against Bitcoin Mining Pools. *Financial Cryptography and Data Security*, **8438**, 72-86. http://dx.doi.org/10.1007/978-3-662-44774-1_6

[45] Kroll, J.A., Davey, I.C. and Felten, E.W. (2013) The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. *The* 12*th Workshop on the Economics of Information Security*, Washington DC, 11-12 June 2013.

[46] Hu, J. and Zambetta, F. (2008) Security Issues in Massive Online Games. *Security and Communication Networks*, **1**, 83-92. http://dx.doi.org/10.1002/sec.5

[47] Ku, Y., Chen, Y., Wu, K. and Chiu, C. (2007) An Empirical Analysis of Online Gaming Crime Characteristics from 2002 to 2004. *Intelligence and Security Informatics*, **4430**, 34-45. http://dx.doi.org/10.1007/978-3-540-71549-8_3

[48] Bardzell, J., Jakobsson, M., Bardzell, S., Pace, T., Odom, W. and Houssian, A. (2007) Virtual Worlds and Fraud: Approaching Cybersecurity in Massively Multiplayer Online Games. *Proceedings of DiGRA* 2007 *Conference*, Tokyo, 24-28 September 2007, 451-742.

[49] Kiondo, C., Kowalski, S. and Yngström, L. (2011) Exploring Security Risks in Virtual Economies. 1*st International Conference on Social Eco-Informatics*, Barcelona, 23-29 October 2011.

[50] Irwin, A.S.M. and Slay, J. (2010) Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft. *Proceedings of the* 1*st International Cyber Resilience Conference*, Perth, 23-24 August 2010, 41-50.

[51] Ministry of Economy, Trade and Industry (2013) Survey on Information Processing in 2012: Result Detail Part 3—Information Security. (In Japanese) http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/h24jyojitsu.html

[52] Ministry of Economy, Trade and Industry (2012) Survey on Information Processing in 2012: Questionnaire. (In Japanese) http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/03_H24chousahyo.pdf

## Appendix A. Poitan.net

Poitan (http://poitan.net) provides information on more than 200 LPs in Japan, such as estimated real-currency values of LP points, exchange/conversion rates between different LPs and how long the conversion would take. Suppose that a consumer would like to convert a certain amount of ANA (All Nippon Airways, a star alliance member) miles, say, 20,000 miles, into JAL (Japan Airlines, a one-world alliance member) miles. In response to this query, Poitan shows some possible conversion routes. For example, on December 25, 2015, Poitan said there were 87 possible routes. One of the possible routes with the best rate was as follows:

1) Convert 20,000 ANA miles (estimated value is 30,000 JPY (Japanese Yen)) into 20,000 JQ Card Points[2] points (estimated value is 20,000 JPY). This would take about 60 days.

2) Convert 20,000 JQ Card points into 20,000 Epos Card Points[3] (estimated value is 20,000 JPY). This would take about 3 days.

3) Convert 20,000 Epos Card Points into 10,000 JAL miles (estimated value is 15,000 JPY). This would take about 60 days.

## Appendix B. Data and Proxies for Empirical Analyses

### B.1. 82 Selected LPs

**Table A1** shows the 82 selected LPs. *LP ID* indicates the LP's ID of Poitan.net. You can access the information of an LP via http://dir.poitan.net/(.*).html, where (.*) is its ID number.

### B.2. Industry

**Table A2** shows the nine industries which operate LPs in Japan.

### B.3. Calculations of the Proxies

Our empirical studies were conducted based on the Gordon-Loeb security investment model [6], which considers the following four parameters as fundamental parameters: *expense*—the amount of security investment, *damage*—the amount of damage when the attack occurred, *threat*—the probability that an attack occurs, and *vulnerability*—the conditional probability that a threat once realized would be successful. When we consider the security of LP systems, one possible interpretation of the four parameters is as follows: *Expense* is the expense on IT security countermeasures by the LP-operating company; *Damage* is the amount of damage from IT incidents; *Threat* is considered to be high if the LP points' liquidity is high because higher liquidity implies more chances of achieving criminal benefits by malicious conversion of LP points or their redemption and it can be a main attractive factor; *Vulnerability* is considered to be lower if the online user authentication system of an LP is implemented in a more secure manner.

This appendix shows how we set and calculate each proxy based on this interpretation, other than *threat*.

#### B.3.1. Damage

As is shown in **Table A3**, METI's numerical data of IT damage represent only the ranges because of its questionnaire design [52]. So we calculated the average damage size for every industry and every capital size level by using the middle value of the range (e.g. 0.75 million JPY for the range "0.5 million to 1 million") with an exception at the edge (*i.e.* we use 200 million JPY for the range "over 100 million." This method is also used by METI [51].

Then, from each LP's industry and capital size, we calculate its damage. We set this damage size as $damage_i$ where $i = 1, 2, \cdots, 82$ indicates each respective LP. For example, if $LP_1$'s industry is "Information Service" and its capital size is "under 50 million JPY", $damage_1 = 1875000$.

This proxy calculation differs from [5] in the following three points. 1) Reference [5] ignored firms which answered "did not suffer information security incidents," but we consider them as zero because it is more accurate. 2) In [5], they calculated the average damage considering only the industrial categorization, but we also considered the capital size for segmentation. 3) Reference [5] used $impact = damage_{IND_i} * rank_i$ as the proxy

[2]JQ Card Point is a reward program of a credit card provided by a Japanese railway company.

[3]Epos Card Point is a reward program of a credit card provided by one of the biggest department store in Japan, Marui.

**Table A1.** List of the 82 Selected LPs (Part 1). LP ID indicates registered ID at Poitan, Industry ID indicates each industry (details are in **Appendix B.2**), and Capital size is each LP operator's capital size. Security score shows a security requirement level calculated by the methods described at **Appendix B.3.3**. N/A means that we cannot access the corresponding information.

| LP ID at Poitan | Name of LP | Industry ID | Capital size (JPY) | Security score |
|---|---|---|---|---|
| 1 | JAL Mileage bank | 20 | 355,845,000,000 | 0.667 |
| 2 | ANA Mileage club | 20 | 25,000,000,000 | 0.667 |
| 15 | Mitsui Sumitomo card | 23 | 34,030,000,000 | 0.667 |
| 29 | G-Point | 19 | 296,000,000 | 0.333 |
| 30 | Net Mile | 19 | N/A | 0.000 |
| 31 | J-Point (changed to "My green stamp") | 19 | 100,000,000 | 0.167 |
| 32 | Outlet Point | 26 | 1,527,000,000 | 0.500 |
| 34 | Biccamera | 22 | 18,402,380,000 | 0.167 |
| 36 | Rakuten | 19 | 1,095,300,000 | 0.000 |
| 38 | Cecile | 22 | 2,000,000,000 | 0.167 |
| 39 | Belle Maison | 22 | 20,359,000,000 | 0.167 |
| 42 | Amazon Gift Voucher | 22 | N/A | 0.000 |
| 43 | T Point | 19 | 100,000,000 | 0.333 |
| 44 | Jbook | 22 | 4,340,000,000 | 0.000 |
| 45 | Honto | 22 | 4,340,000,000 | 0.000 |
| 46 | NTT Docomo | 17 | 949,679,500,000 | 1.000 |
| 47 | au | 17 | 141,851,000,000 | 1.000 |
| 48 | NTT communication | 17 | 211,700,000,000 | 1.000 |
| 62 | Ponta | 26 | 2,381,578,000 | 0.500 |
| 63 | Mitsubishi Tokyo UFJ Bank | 23 | 1,711,900,000,000 | 0.667 |
| 66 | Manex Stock Company | 23 | 12,200,000,000 | 0.833 |
| 70 | Starbucks Card | 22 | 8,548,090,000 | 0.333 |
| 71 | Matsumoto Kiyoshi | 22 | 21,086,000,000 | 0.500 |
| 74 | Rakuten Edy | 19 | 1,840,000,000 | 1.000 |
| 78 | Risona Bank | 23 | 50,400,000,000 | 1.000 |
| 81 | Yamada Denki | 22 | 71,050,000,000 | 0.000 |
| 92 | Recruit | 26 | 10,000,000,000 | 0.000 |
| 97 | Sony Finance | 19 | N/A | 1.000 |
| 98 | Sony point | 9 | 100,000,000 | 0.167 |
| 100 | Daiwa Stock Company | 23 | 100,000,000,000 | 1.000 |
| 101 | Circle K Sunkus | 22 | 8,380,400,000 | 0.000 |
| 103 | Chobi Rich | 26 | 65,700,000 | 0.167 |
| 110 | ANA JCB Card | 23 | 10,616,100,000 | 0.800 |

**Continued**

| | | | | |
|---|---|---|---|---|
| 123 | Sofmap | 22 | 100,000,000 | 0.167 |
| 126 | Bidders | 19 | 10,397,000,000 | 0.167 |
| 127 | Softbank Mobile | 17 | 177,251,000,000 | 0.600 |
| 131 | Web Money | 19 | 495,784,000 | 1.000 |
| 133 | Icoca | 20 | 100,000,000,000 | 0.667 |
| 134 | J-WEST Card | 20 | 100,000,000,000 | 0.667 |
| 138 | Times | 26 | 8,219,000,000 | 0.167 |
| 146 | PeX | 19 | 198,000,000 | 0.167 |
| 148 | nanaco | 23 | 7,500,000,000 | 0.500 |
| 149 | nanaco Point | 23 | 7,500,000,000 | 0.500 |
| 152 | Suica point club | 20 | 200,000,000,000 | N/A |
| 155 | Chocom e Money | 17 | 306,578,542 | 0.000 |
| 158 | Tepore | 17 | 270,000,000 | 0.000 |
| 159 | Chocom point | 17 | 306,578,542 | 0.000 |
| 160 | JP BANK Card | 23 | 3,500,000,000,000 | 0.833 |
| 161 | Point Monkey | 26 | 80,000,000 | 0.167 |
| 163 | Central Nippon Expressway Company | 20 | 65,000,000,000 | 1.000 |
| 164 | SBI Point | 23 | 81,681,000,000 | 0.000 |
| 171 | MUFG Card | 23 | N/A | 0.667 |
| 200 | ENEOS Card | 22 | 139,400,000,000 | 1.000 |
| 206 | Kaetoku card | 19 | N/A | 1.000 |
| 208 | Cue Monitor | 19 | N/A | 0.167 |
| 209 | NTT East Japan (Flet internet) | 17 | 335,000,000,000 | 1.000 |
| 211 | Point Exchange | 19 | 411,162,000 | 0.000 |
| 212 | Gendama | 19 | 411,162,000 | 0.167 |
| 215 | Apple World | 26 | 200,000,000 | 0.000 |
| 217 | nimoca | 20 | 126,400,000 | 1.000 |
| 227 | TEPCO | 16 | 1,400,900,000,000 | N/A |
| 232 | GetMoney! | 26 | 211,500,000 | 0.000 |
| 237 | Saitama Risona Bank | 23 | 70,000,000,000 | 1.000 |
| 238 | MyVoice | 19 | 178,000,000 | 0.000 |
| 239 | Chance It | 19 | 211,500,000 | 0.000 |
| 240 | Ikyu | 19 | 914,000,000 | 0.000 |
| 241 | Fastask | 19 | 10,146,510,000 | 1.000 |
| 242 | Ogaki Kyoritsu Bank | 23 | 36,100,000,000 | 1.000 |
| 244 | Juroku Bank | 23 | 36,800,000,000 | 0.400 |

**Continued**

| | | | | |
|---|---|---|---|---|
| 246 | Ikeda Senshu Bank | 23 | 50,700,000,000 | 1.000 |
| 248 | Kinki Osaka Bank | 23 | 389,071,000,000 | 1.000 |
| 253 | For Travel | 19 | 915,984,000 | 0.000 |
| 255 | Tokopo | 20 | N/A | 0.500 |
| 259 | POINT-BOX | 19 | 10,000,000 | 0.000 |
| 261 | East Nippon Expressway Company | 20 | 52,500,000,000 | 1.000 |
| 262 | Apa Hotel | 26 | 1,912,000,000 | 1.000 |
| 273 | E Tour | 26 | 260,500,000 | 0.167 |
| 284 | Go to Dentist! | 26 | 13,000,000 | 0.167 |
| 286 | Boox Store | 22 | 310,100,000 | 0.000 |
| 296 | ANA Sky Coin | 20 | 25,000,000,000 | 0.667 |
| 303 | QooPo | 13 | 28,534,000,000 | N/A |
| 307 | My Acuvue | 22 | 8,000,000,000 | 0.333 |

**Table A2.** Nine industries which operate LPs in Japan. Each industry ID is the same as in [5].

| Industry ID | Industry Name |
|---|---|
| 09 | Manufacturing and electrical machinery, equipment and supplies |
| 13 | Miscellaneous manufacturing industries |
| 16 | Electricity, gas, heat supply and water |
| 17 | Video picture, sound information, broadcasting and communications |
| 19 | Information services |
| 20 | Transportation and postal activities |
| 22 | Retail trade |
| 23 | Finance and insurance |
| 26 | Miscellaneous non-manufacturing industries |

of damage, where $IND_i$ indicates $LP_i$'s belonging industry ID, $damage_i$ is the average damage amount of its industry and $rank_i$ indicates the LP's ranking score at Poitan.net. However, this might be somewhat artificial.

### B.3.2. Expense

The proxy of expense is also calculated from METI's data by the same method used for the damage. Then, $expense_i\ (i = 1, 2, \cdots, 82)$ is set.

### B.3.3. Vulnerability

The metric of vulnerability is the same as [5] used. We used six requirements in the registration process, the authentication (login) process, and the back-up authentication process of each LP. **Table A4** shows these six requirements. They computed the security score, $sec\_score_i$, of $LP_i$ as the ratio of "the number of satisfied requirements in $LP_i$" to "the number of requirements about which we can obtain data regarding $LP_i$."

$sec\_score_i$ represents how unsuccessful an attack is, so we can view $sec\_score_i$ as a metric for *anti*-vulnerability.

**Table A3.** Examples of METI's data about the IT damage amount [51].

| | Capital Size (JPY) | Total # of Firms | # of responded firms | Damage from incidents (JPY) | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Under 0.5 million | 0.5 million to 1 million | 1 million to 1.5 million | 1.5 million to 2 million | 2 million to 4 million | 4 million to 6 million | 6 million to 8 million | 8 million to 10 million | 10 million to 15 million | 15 million to 20 million | 20 million to 30 million | 30 million to 50 million | 50 million to 100 million | Over 100 million | Not sure | Did not suffer |
| | | | | # of firms | # of firms | # of firms | # of firms | # of firms | # of firms | # of firms | # of firms | # of firms | # of firms | # of firms | # of firms | # of firms | # of firms | # of firms | # of firms |
| Information Service | under 50 million | 69 | 10 | 3 | 1 | - | - | - | - | - | - | - | - | - | - | - | - | 2 | 4 |
| | 50 million to 100 million | 132 | 26 | 9 | 2 | - | - | 1 | - | - | - | - | - | - | - | - | - | 2 | 12 |
| | 100 million to 300 million | 48 | 10 | 3 | 1 | 1 | - | - | - | - | - | - | - | - | - | - | 1 | 2 | 2 |
| | 300 million to 500 million | 26 | 9 | 4 | 1 | - | - | - | - | - | - | - | - | - | - | - | - | 3 | 1 |
| | 500 million to 1 billion | 18 | 6 | 4 | - | - | - | - | - | - | 1 | - | - | - | - | - | - | - | 1 |
| | 1 billion to 10 billion | 39 | 15 | 5 | 1 | - | - | 1 | - | - | - | 1 | - | - | - | - | - | 3 | 4 |
| | over 10 billion | 8 | 3 | 1 | - | - | - | - | - | - | - | 1 | - | - | - | - | - | - | 1 |
| | unknown | 1 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | Total | 341 | 79 | 29 | 6 | 1 | - | 2 | - | - | 1 | 2 | - | - | - | - | 1 | 12 | 25 |
| Transportation and postal activities | under 50 million | 65 | 5 | 3 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 2 |
| | 50 million to 100 million | 113 | 10 | 3 | 1 | - | - | - | - | 1 | - | - | - | - | - | - | - | - | 5 |
| | 100 million to 300 million | 30 | 4 | 3 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 1 |
| | 300 million to 500 million | 19 | 1 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 1 | - |
| | 500 million to 1 billion | 10 | 1 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 1 | - |
| | 1 billion to 10 billion | 34 | 5 | 1 | - | - | - | - | - | - | - | - | - | - | - | - | - | 2 | 2 |
| | over 10 billion | 15 | 6 | 2 | - | - | - | - | - | - | - | - | - | - | - | - | - | 2 | 2 |
| | unknown | 1 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | Total | 287 | 32 | 12 | 1 | - | - | - | - | 1 | - | - | - | - | - | - | - | 6 | 12 |

**TableA4.** Security requirements in web authentications used for the calculationof *sec_score* [5].

| Process | Requirements |
|---|---|
| Registration | - Trusted information (e.g. certified information, security code, information which is matched to certifiable document).<br>- Necessity of physical card or account.<br>- Implementation of additional security techniques (e.g. CAPTCHA, secret question). |
| Authentication (login) | - Data which increases difficulty to log into the account. (e.g. mobile number, physical card number, system generated ID). |
| Back-up authentication | - Trusted information. |
| (password recovery) | - Physical card or account number. |

### B.3.4. Normalization

Reference [5] did not normalize any parameters, but we normalize *damage* and *expense* with *capital size* as follows:

$$\text{damage:}\quad \log\left(damage_i\right)/\log\left(capital\_size_i\right),$$

$$\text{expense:}\quad \log\left(expense_i\right)/\log\left(capital\_size_i\right).$$

Each LP-operating company has a lot of IT systems, and an LP system is just one of them. Since the empirical data of expense and damage is for all the IT systems of the company, some normalization would be necessary when we measure the expense and expense on its LP system.

## Appendix C. Liquidity Definition at the Previous Research

We briefly describe how Jenjarrussakul and Matsuura [5] defined *liquidity* and used this metric.

Before they conducted quantitative analysis, they first considered the LPs security issues by industry. They listed 204domestic LPs and classified them into 9 industries. They drew a graph of the Japanese LP partnership network where each node indicates an industry. Since they were interest in how each industry node is connected, they checked the edge types—one-directional, opposite one-directional, or bidirectional—between industries and the average number of connecting LPs of all the LPs belonging to each industry.

In order to quantitatively examine which industry is more willing to connect with other industries via LP, they introduced a metric *liquidity* as a multiplier of the number of edge types, $x$, and the average number of partners regarding the LPs in a node, $y$:

$$liquidity = x * y\ .$$

Then, using METI's data, they discussed the relation between liquidity and damage or security investment in the industry-wise level.

After this industry based discussion, they entered upon a LP divided discussion and carried on quantitative empirical analysis with the same liquidity definition above. However, this definition does not seem suitable and intuitively convincing when we consider how easily attackers convert the points into actual monetary profit when we consider the LP-wise situation divided from the industry-wise cluster.